General Information

Policy Name:	HIPAA Information System Activity Review
Category:	Risk Management
Applies To:	All Staff
Key Words:	ePHI, PHI, Access, Security Management
Associated Forms & Policies:	HIPAA: Sanction (P0587)
Original Effective Date:	04/01/12
Review Dates:	01/20/16, 10/23/17, 10/14/22, 10/17/23, 10/17/24, 10/15/25
Revision Dates:	10/25/19, 10/19/21
This Version's Effective Date:	10/19/21

Policy

Applications/systems that access, store, and/or transmit electronic Protected Health Information (ePHI) should have the capabilities necessary to review all access traffic, etc. to ensure all data remains confidential and secure. Crouse Hospital has the responsibility to ensure these mechanisms are in place and are utilized on a regular basis to ensure all patient data remains secure and that any potential HIPAA access violation is discoverable.

The Hospital will take reasonable steps to ensure that any information systems containing ePHI will have enabled any available auditing mechanisms for the purpose of activity and event monitoring. Crouse Hospital should review information systems activity including, but not limited to, audit logs, access reports and security incident tracking reports wherever necessary.

Application/system events should be included in any system activity review. Events should include, but are not limited, to the following:

- Monthly Electronic Medical Record (EMR) system audits
- VIP medical record access
- Access to restricted information (ex: substance abuse patients)
- Use of privileged accounts
- Authentication failures
- Use of audit software or utilities
- Potentially security incidents

Crouse Hospital will have designated workforce member(s) who will be responsible for regularly reviewing activity recorded or logged on information systems containing ePHI. The following factors should be considered in determining the frequency of the activity review:

- Risk Analysis findings and recommendations
- Sensitivity of ePHI stored
- Extent to which the information system is connected to other systems

- Significance of applications that exist on the information systems (ex. Tier 1 applications will take precedence due to importance and size of patient data stored within the system)

System activity reviews are only possible with the tools that are available within that system. If a system does not have the mechanisms or capabilities in place to perform a review or audit, Crouse Hospital will utilize any other tools or resources in place (including working with the vendor of the system) to ensure all avenues have been reviewed before determining that a review or audit cannot take place.

Any application/system that has the mechanisms in place to perform a system activity review are subject to reviews at the discretion of the Hospital; **employees should have no expectation of privacy in regards to their access within Hospital systems.**

If a system activity review is conducted and a violation has occurred, Crouse Hospital will move forward with the necessary response and/or sanctions, including possible termination. Refer to the Employee Handbook as well as the HIPAA Sanction policy for more information.

Activity reviews and reports for each information system will be retained for a period of six years.

Procedure

If a system activity review is requested and/or mandated, the following will occur:

1. A review of the request to determine if an audit or report is necessary.
2. If yes, then a designated system employee will review the activity in question.
    a. This employee will most likely be a member of Information Technology (IT) or Risk Management.
3. The designated employee will gather the findings and deliver it to the department/designated individuals assigned to this request.
4. If any violations are discovered, reasonable actions will be taken per the Employee Handbook and HIPAA Sanction Policy requirements.
5. If no violation is found, the department/designated individuals will be notified of these findings.
6. The findings, audit, and/or report will be retained within Risk Management for record-keeping purposes.

References

HIPAA Security Rule 45 CFR § 164.312(b) – Audit Controls

HIPAA Security Rule 45 CFR § 164.308(a)(1)(ii)(D) – Information System Activity Review

HIPAA Security Rule 45 CFR § 164.316 – Policies and procedures and documentation requirements

CMS Minimum Security Requirements – Acceptable Risk Safeguards

Definitions

Electronic Protected Health Information (ePHI):
Electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual.

Access:
The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Addendums, Diagrams & Illustrations

Not Applicable